THE PRICE OF CONVENIENCE:

COMMUNICATIONS, CYBER RISK, AND CYBERSECURITY PRACTICES OF CORPORATE BOARDS

NYSE Governance Services

Diligent

INTRODUCTION

OVER THE PAST decade, the issue of cybersecurity has increasingly gained attention in boardrooms around the world, adding yet another critical topic to already packed board agendas. Cyber risk, which has always represented a significant area of enterprise risk, is finally being acknowledged as intersecting with other areas of the board's oversight, including strategy, operations, and legal, financial, and reputational risks. Yet, while more directors now recognize that their company's cyber risk management strategy is an area of board concern, many directors lack the necessary expertise to feel fully confident in navigating cybersecurity issues.

Meanwhile, digital technology has become the norm in more than half of all corporate boardrooms, with broad consensus that it has eased the burden of director communications, especially for board members who have other full-time commitments, hold multiple board seats, and travel frequently. Additionally, the majority of directors in our survey (55%) report that the use of such technology has increased the overall security of board information. However, even using secure digital board software does not eradicate cyber risk from board communications, nor does it absolve directors from the need to understand, mitigate, and monitor related cybersecurity issues.

Along these lines, many companies struggle with striking the right balance between convenience and security with regard to the distribution of board materials. In January 2017, NYSE Governance Services, in partnership with Diligent Corp., conducted a survey of more than 350 corporate directors of publicly traded companies to gain a better understanding of current board communications practices. The survey's focus was threefold:

① to determine how companies safeguard board communications, while still maintaining a high level of effectiveness;

② to ascertain the current level of awareness and readiness of corporate directors to navigate related cybersecurity issues; and

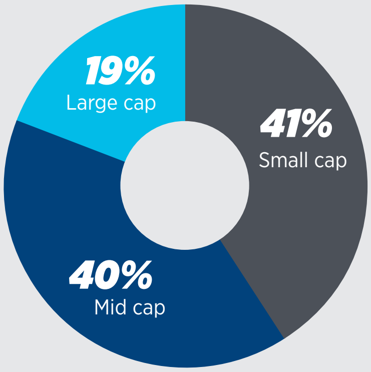
③ to identify potential areas for improvement in managing and mitigating the cyber risks of board communications.

This report provides a summary of the key findings from the survey data, as well as some recommendations for companies to improve their cybersecurity practices related to board communications.

METHODOLOGY

In January 2017, NYSE Governance Services and Diligent teamed up to survey directors of publicly traded companies on their current communications practices, level of cyber risk awareness, and related cybersecurity issues. The survey received 381 responses from directors representing a wide range of industries and company sizes.

MARKET CAPITALIZATION



TITLE (Role on the board)

46%	Outside director
30%	Committee chair
9%	Board chair
8%	Lead director
5%	Executive/Inside director
2%	Other

INDUSTRY

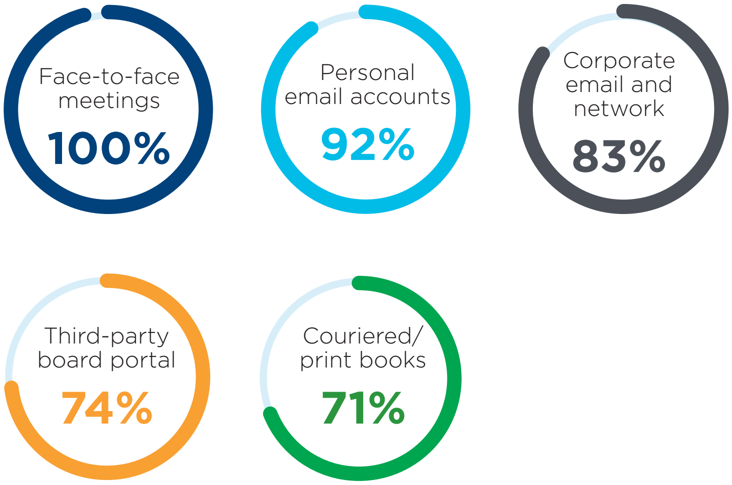
Financials	23%
Industrials	17%
Health care	10%
Information technology	10%
Real estate	9%
Consumer discretionary	8%
Energy	8%
Materials	5%
Consumer staples	4%
Utilities	4%
Telecommunication services	3%

DIRECTORS’ USE OF PERSONAL EMAIL

UPHOLDING THE FIDUCIARY obligations directors have to their companies’ shareholders has become an increasingly complex job. The quantity of information directors receive and absorb to perform the fiduciary role creates communications challenges, both within and outside the boardroom. For most businesspeople, email is still the most common communications channel, but our survey revealed that nine out of 10 directors use an unsecured personal email account (such as Gmail, Yahoo Mail, or Outlook.com) at least occasionally to communicate with fellow directors and management, making it the second most common method of director communication, behind face-to-face meetings (Figure 1). Nearly 60% of directors report they regularly use personal email to communicate with fellow directors.

While our survey did not evaluate the content of directors’ emails being sent through personal email accounts, some respondents commented that they only use personal email accounts to send and receive nonconfidential board information, such as messages regarding meeting scheduling and agendas.

FIGURE 1
DIRECTORS’ PREFERRED METHODS OF COMMUNICATION



DIRECTORS SAY:
“I think all directors, executives, and third parties need to exercise as much care in their electronic communications as they would in a legal document.”

PERSONAL EMAIL: TOO RISKY FOR BOARD BUSINESS

Personal email accounts—like any other unencrypted, or ill-encrypted, digital gateway—can be used as a point of entry into a person’s computer, tablet, or device. If this point of entry is compromised, it endangers all stored materials therein, regardless of the channel through which these materials were originally received. Likewise, directors’ personal emails live outside the corporate firewall where they cannot be managed or archived by the corporate secretary in accordance with the company’s record retention policy. Additionally, because personal email is not a “closed-loop” system, using this channel for director communications invites the risk that a director might accidentally send sensitive information to unintended recipients.

RECOMMENDED ACTION STEPS

Dottie Schindlinger, governance technology evangelist at Diligent, says directors should consider implementing a closed-loop, secured, and controlled messaging system, preferably one that is integrated with the company’s existing secure board portal system. “What directors might sacrifice in convenience by not using personal email,” she explains, “they gain in cybersecurity, mitigation of cyber risk, and reduced personal liability.” She indicates that secured, director-focused messaging apps exist that allow directors to communicate as easily as texting, including the ability to add attachments, communicate with individuals or groups of directors (e.g., a single committee, board officers), archive/retain communications, and remotely wipe communications from personal devices in the event the device is lost or stolen.

DOWNLOADING/STORING BOARD MATERIALS

Visiting activity of the Web-site by hours
Worldwide customers activity
Web-site traffic

TODAY'S DIRECTORS have a dizzying array of competing demands. Inside directors have the day-to-day pressures of being top executives in their companies, while also having to meet the requirements of serving on a board. Many outside directors serve on multiple boards and have to delineate the performance, health, and risk profiles of each enterprise. Most directors keep busy travel schedules and are often forced to prepare for an impending board meeting on their mobile devices as they dash through airports and train stations. Having a simple way for directors to access board and committee materials—through a secure, digital platform, using any mobile device, offline or online—becomes critical to success.

In this context, it's not too surprising that half (49%) of the survey respondents acknowledge it is common practice for board members to download board meeting materials, reports, and other company documents onto personal computers and devices, where they can be accessed quickly and offline (Figure 2). Depending on the communication method used, downloading documents onto personal devices does not need to entail storing documents outside a secured and controlled environment. Some board software platforms permit offline access to documents without allowing those documents to leave the confines of the app. Nevertheless, our data uncovered that 22% of respondents are saving/storing board materials on personal or external drives, outside of a secured environment (Figure 3).

Most directors recognize that the practice of storing sensitive information outside the company's firewall and control represents risk, although some may not realize how great a risk this practice represents. Nearly half (47%) of respondents, however, agree the move to digital file sharing has increased the risk of improper handling of sensitive information, and their comments indicate better guidance might be desired.

FIGURE 2

HOW OFTEN DO YOU DOWNLOAD BOARD BOOKS OR COMPANY DOCUMENTS ONTO YOUR PERSONAL COMPUTER OR DEVICES FOR EASIER ACCESS?

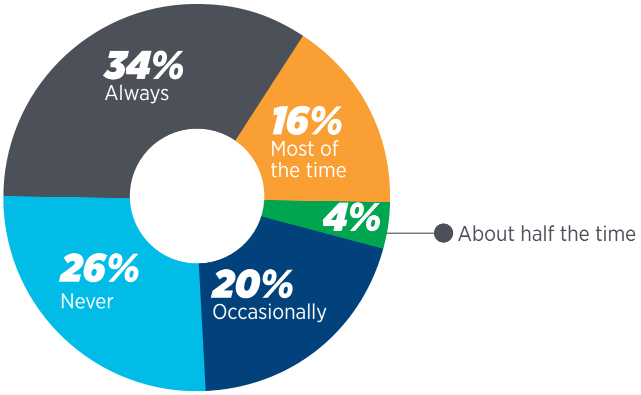
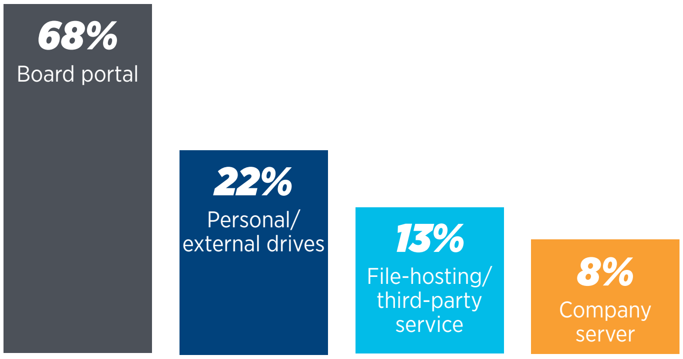


FIGURE 3

WHERE DO YOU TYPICALLY STORE YOUR DIGITAL BOARD MEETING MATERIALS?



DIRECTORS SAY:

"[Our] board does allow files on the portal to be downloaded to a director's personal device. I only [do] this if something comes late, and I want to be able to look at it while flying to the meeting. As it's the same document as on the portal, I don't consider it a risk..."

OUTSIDE THE FIREWALL, INSIDE THE FIRING LINE

It's not surprising to learn that many directors not only download board documents to personal devices and drives, but also store files there long term. This practice may have been born out of necessity due to directors' hectic travel schedules and the need to have offline/ready access to documents while in transit. Yet, this reality increases the risk and breadth of consequences associated with a personal device being lost, left on board in a seat pocket, stolen from a restaurant table, or left on the X-ray belt at a security checkpoint. "Meanwhile, unless the director uses mobile device management, there might be no way to remotely wipe the contents off the lost device," explains Schindlinger, adding that depending on the kind of data on the device, the event could be considered a "reportable incident," triggering a requirement to disclose the data breach to any potentially affected parties.

RECOMMENDED ACTION STEPS

According to Diligent experts, the above situation is what makes secure board management software apps shine, as many such apps allow for secure offline access to files without leaving the confines of the app. "Access to the app can be controlled externally by the director (by logging in on another device) or by an administrator and can allow for biometric logins, two-factor authentications, and password complexity to increase the security of offline data. Many board management apps provide a way to remotely wipe data from the app, helping ensure that a lost device does not equal a data breach," notes Schindlinger.

BOARD COMMUNICATIONS SECURITY AND OVERSIGHT

ONE BEST PRACTICE often noted by data security experts is for the company's internal data security professionals—chief officers of information security (CISO, CSO), compliance (CCO), and IT (CIO)—to verify that sensitive materials, if downloaded, are saved to a folder/app over which the company retains control. In almost every other case where a company executive needs to save sensitive information to a device, they would likely be required to save documents only to company-controlled secure apps, secure cloud-based file storage systems, or password-protected folders on the company's hard drive. This helps reduce the vulnerabilities of using personal devices to access secure data and ensures that the data security team can fulfill its obligation to provide oversight of access to sensitive company documents.

Despite this norm, when it comes to directors and board documents, only 8% of our respondents report that their company's IT, IS, or data security team has any role in sanctioning or authorizing the board's methods of communication; rather, 27% relegate this responsibility to the board chair or lead director (Figure 4).

FIGURE 4
SANCTIONING AUTHORITY VS. ADMINISTRATOR

	Sanctions	Administers
Audit or risk committee	**16%**	**3%**
Board chair or lead director	**27%**	**5%**
Investor relations team	**4%**	**6%**
IT, IS, or data security team	**8%**	**20%**
Legal or corporate secretary	**15%**	**28%**
No one	**6%**	**1%**
Don't know	**5%**	**0%**

THE RISK OF E-DISCOVERY

BEYOND THE RISK of data theft and the potential compromise of confidential information, there is another consequence to using personal systems to conduct board business. The Delaware Courts, among others, have held that all electronically stored information relating to the business or acquired during the course of conducting business—including documents, text messages, and emails—is the property of the employer and is therefore "discoverable" during litigation. According to the Delaware Court of Chancery, a document's purpose, rather than its source, determines whether it will be deemed discoverable.

In other words, directors who use personal email accounts, devices, and computers to conduct business may subject themselves to searches of their private files, phones, and emails if litigation ensues. For their own sake, as well as to protect the company, board members should comply with their company's document retention policy for the storage and destruction of records, including those received via personal accounts and retained on personal drives.

In addition, by allowing this practice to continue unrestricted, directors may be held liable for neglecting their fiduciary duty of care by putting confidential information at risk, especially if it is established that there were more secure means of communications at their disposal.

To mitigate these risks, directors and their executive team are advised to take a hard look at the board's communications practices and implement the right measures to protect themselves against both litigation and loss stemming from cyberattacks.

One way to undertake such an evaluation is by undergoing an audit of directors' current communications practices to identify areas of risk that could lead to loss and then benchmark those practices against the corporate community at large. Finally, with guidance from the company's information security team, the board should formally adopt a communications policy that clearly outlines acceptable devices, methods, competencies, and practices. This policy should be accompanied by training, provided at least annually, as well as occasional auditing of directors' practices.

CYBERSECURITY AUDITING AND TRAINING FOR DIRECTORS

GIVEN THE LARGE NUMBER of well-publicized data leaks and cyberattacks that have occurred recently on companies in every industry, it's no surprise that directors report an increased concern over cybersecurity. Several respondents commented either that cybersecurity already is a key focus area for the board, or that it should be.

Increased interest in cybersecurity, however, has not yet led to routine security auditing of director communications. In our study, we learned that four out of 10 directors are unaware that any security audit of their communications practices has ever taken place (Figure 5). Half say they don't know whether their security teams monitor the board's adherence to corporate communications guidelines. About one-quarter (23%) confirm such monitoring of communications practices is nonexistent at the board level (Figure 6).

Some companies require board members to undergo cyber training alongside other company employees. However, almost two-thirds (62%) of directors in our survey report not being required to undergo cybersecurity training at all (Figure 7). Only 9% confirm they were required to take the same training as all company employees, and 23% say they are only asked to do so once during their tenure (Figure 8). With many of the company's key assets at risk, we will be watching this area closely to determine if more companies begin to include board members in this important compliance and training area.

FIGURE 5

HAS YOUR BOARD EVER CONDUCTED A SECURITY AUDIT OF ITS COMMUNICATIONS PRACTICES?

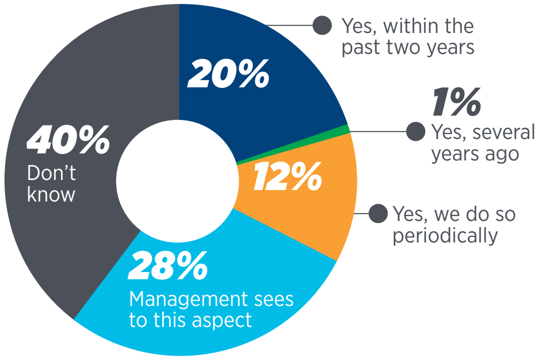


FIGURE 6

DOES YOUR SECURITY TEAM MONITOR THE BOARD'S ADHERENCE TO CORPORATE COMMUNICATIONS GUIDELINES?

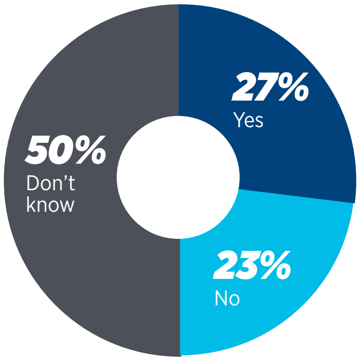


FIGURE 7

IS YOUR BOARD REQUIRED TO UNDERGO CYBERSECURITY TRAINING?

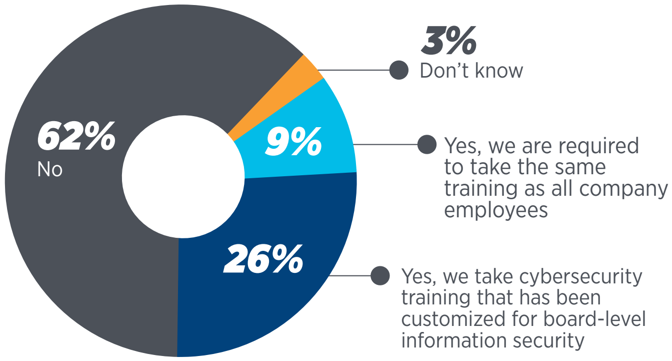
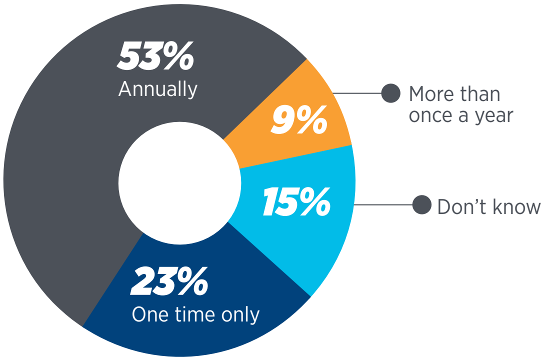


FIGURE 8

HOW OFTEN ARE YOU REQUIRED TO UNDERGO TRAINING?



DIRECTORS SAY:

"From my discussion with board members across a number of boards, I think companies need to think more intentionally about having IT support and IT security measures in place for board members as many are do it yourself for IT purposes and do not have a background in the area."

BOARD INFORMATION SECURITY IS A MOVING (HIGH-VALUE) TARGET

It's a bit perplexing that the auditing of board communications, accompanied by cybersecurity training for directors, has not yet become routine. At most companies, board members are on the front lines of a pitched battle; directors are targeted for cyberattack precisely because they have access to the most sensitive information with the least amount of oversight. Because cyber risk and communication technology involve changes that occur very rapidly, it's important to have someone with ongoing expertise in this area help with the evaluation process. But with so many hands in the cybersecurity pot—CISOs, IT managers, compliance officers, board members, outside professionals—it's legitimate to ask who has ultimate responsibility for risk mitigation? In almost any other context, the responsibility for data security is part of the information security officers' purview. Even if the board includes several outside directors, it should be required to adhere to similar communications practices and standards as the company's employees. The business risk inherent to director communications is too great to be ignored.

RECOMMENDED ACTION STEPS

Experts agree, the company's information security officers should provide a similar level of oversight, cyber risk auditing, and cybersecurity training for directors as for the rest of the company, and a director's ability to adhere to proper procedure should be considered a basic standard for continued membership on the board. Diligent's Schindlinger maintains the security team should be involved in selecting, configuring, and authorizing the secure communications software platform being used by the board, in addition to weighing in on specific policies and procedures governing the appropriate use of personal devices, and ensuring data can be remotely wiped from devices in the event of loss or theft. "Cybersecurity training and testing should become a routine part of the board's calendar," she advises. "Testing might include table-top exercises led by the CISO at a board meeting to role play what would happen in the event of a breach of board communications; or targeted tests, such as fake spear phishing attacks, might be performed." She recommends a summary report then be presented at the next board meeting with follow-up training and a second audit conducted if needed. Likewise, directors should be encouraged (and rewarded) for helping one another adhere to secure communications practices. Should they spot a fellow director doing something outside the bounds of the security policy, Schindlinger suggests they take a personal stake in helping the director improve and alert the security team of any potential threats or risks.

SECURITY VS. CONVENIENCE: A DELICATE BALANCING ACT

THERE EXISTS AN INVERSE RELATIONSHIP between security and convenience—the more secured a system becomes, the less convenient it is for the user to access. Our survey revealed this ongoing and underlying tension surrounding secure board communications. Several respondents voiced frustration at trying to reconcile the goals of security with their own convenience, particularly when it comes to board documents. Some believe extra layers of security and a more rigorous process could hinder their ability to perform their duties effectively. This fear, combined with a more generalized apprehension to technology in general, alongside the time crunch most directors and executives face, provides strong incentive to make board communications as simple and unencumbered as possible.

Directors who serve on multiple boards report finding it burdensome to log in to multiple company-issued devices or systems to conduct their business, and therefore have switched to personal email, personal devices, or printed materials instead. Yet, others feel that directors' resistance to using technology appropriately only perpetuates the stereotype that directors are out of step with the cyber realities of the world within which their companies operate.

One solution to this balancing act in recent years has been the widespread adoption and use of secure board management software platforms, or board portals, which are an increasingly popular means of connecting directors and management. These systems provide a controlled environment where board books, policies, minutes, reports, and other company documents

DIRECTORS SAY:

"With all the concerns of current board members being of the pre-digital age, it is disconcerting when I see a member with a big three-ring binder. I think it simply sends the wrong signal."

"[I'm] becoming more and more frustrated with issues related to convenience vs. security. Back to voice only?"

"Personally, I'm about half won over to receiving board materials digitally. Even with the ability to add notes to a digital board book, I generally prefer hard copy to improve my preparation and participation in board or committee meetings."

are distributed securely to directors' mobile devices and computers. Board portals also provide the ability to annotate and edit files without having to print or download them to an unsecured location. There are directors, however, who confessed hesitation to engaging in some aspects of an all-digital environment. "I find it very difficult to read long reports or spreadsheets online," commented one director who prefers to print out the documents in advance of meetings.

Yet, most board members in our study report having a very positive experience with the move to digital board communications. In fact, almost three-quarters (74%) say they use external board portals, speaking to these platforms' ability to ease regular communications and boost security. "[A board portal] provides better security than personal email accounts or paper," observed one respondent. "It is more efficient since all materials are available in one place, including materials from past meetings. There was concern among management that a few board members would not embrace the technology. This was resolved by one-on-one training and by providing iPads to the few board members who didn't have them."

Nevertheless, the use of board portals requires a certain discipline on the part of the executive team, who may find it easy to use the platform as a data dumping ground. Our survey found that the use of board portals has increased both the frequency and volume of board communication (Figure 9). By the same token, some directors are tempted to request more detail than is necessary to perform their oversight role. In either case, the temptation to overload the digital board book should be tempered with the realization that excess material can be just as harmful to proper oversight as a dearth of information.

FIGURE 9

HOW HAS DIGITAL TECHNOLOGY INFLUENCED THE WAY MANAGEMENT COMMUNICATES AND SHARES INFORMATION WITH YOUR BOARD?

	Increased	Decreased	Stayed the same
Frequency	↑**65%**	↓**0%**	–**35%**
Relevance	↑**40%**	↓**2%**	–**58%**
Security	↑**55%**	↓**9%**	–**36%**
Volume	↑**52%**	↓**3%**	–**45%**

FIGURE 10

WHICH OF THE FOLLOWING BEST CHARACTERIZES BOARD MEETING MATERIALS YOU RECEIVE FROM MANAGEMENT?

Too much detail; not enough summary highlights	The right mix of summary highlights and accompanying detail	Not enough detail; too reliant on summary highlights
15%	**81%**	**4%**

While roughly two-thirds (65%) of directors note a heightened frequency of communications and more than half (52%) report an increase in volume, our study found that eight out of 10 directors believe they receive the right mix of summary highlights and accompanying detail from management (Figure 10).

These findings are an indication of where digital board communications tools should continue to be developed. Schindlinger notes that to date, most companies have used board management software simply to replace what they used to do via paper, that is to provide reports, minutes, agendas, and other documents to directors in preparation for quarterly meetings. "While this approach adds measures of security, control, and convenience," she observes, "it hasn't yet changed the paradigm of what the board knows and how current they are on company performance." In other words, board software has not yet changed the way the board learns. "We envision a future where board management software strives to help the board become smarter about the present, not just more efficient at reviewing the past." Or, as one director remarked, "There is so much uncertainty in today's markets that the communications process needs to be more fluid."

In sum, directors want better access to key metrics on company performance, health, areas of risk, and potential opportunities, all provided closer to real time and in a quickly digestible, visually appealing format. While this is not yet a reality, the technology exists to make it so, and directors have voiced their desire to have this kind of insight in a simple, easy-to-use fashion.

CONCLUSION: WHERE DO WE GO FROM HERE?

IT IS WELL KNOWN that the greatest source of risk in any technology is created when people use the system. Directors and executives who lack cyber risk awareness, are not receiving proper training and oversight, or are careless in their practices account for the most common causes of corporate cyber incidents. In this digital world, the board's communications practices have the potential to make the company vulnerable to data breaches, leaks, litigation, regulatory fines, sanctions, and financial or reputational losses.

Directors must therefore increase their understanding of the risks involved in using methods that receive no oversight by the company's information security team, as well as embrace the fact that information security must take precedent over practicality. This means the board and executive team should work together to ensure enough time and resources are devoted to selecting, implementing, and monitoring a company-supported infrastructure that features highly secure methods of communication in a convenient and effective format for busy directors. With liability increasing at every turn, as a best practice, outside directors should adhere to the same IT security protocols that apply to regular employees, including undergoing regular cybersecurity training, testing, and audits.

In the end, cyber awareness begins and ends at the top. Better informed and educated board members set the tone for the entire organization, and despite the advances of communications technology, directors must be extremely conscientious in observing proper procedures, adhering to compliance rules, and exercising good cyber oversight. Diligent and NYSE Governance Services are committed to reporting on trends and offering analysis in this area to help board members ensure they are doing all they can to safeguard their company and themselves from cyber liability.

In the end, cyber awareness begins and ends at the top. Better informed and educated board members set the tone for the entire organization.

Diligent

Diligent is the leading provider of secure corporate governance and collaboration solutions for boards and senior executives. Over 4,700 clients in more than 70 countries and on all seven continents rely on Diligent to provide secure, intuitive access to their most time-sensitive and confidential information, ultimately helping them make better decisions. The Diligent Boards solution speeds and simplifies how board materials are produced, delivered, and collaborated on via any device, removing the security concerns of doing this by courier, email, and file sharing. Visit www.diligent.com or follow us on Twitter @diligentHQ to learn more.

NYSE Governance Services

NYSE Governance Services is an integrated suite of resources for public and privately held companies worldwide seeking to create a leadership advantage through corporate governance, risk, ethics, and compliance practices. NYSE Governance Services offers a range of training programs, advisory services, benchmarking analysis and scorecards, exclusive access to peer-to-peer events, and thought leadership on key governance topics for company directors and C-level executives.

NYSE Governance Services firmly believes that businesses run ethically enjoy greater long-term success, ultimately promoting stronger capital markets. For more information on NYSE Governance Services, please visit www.nyse.com/governance.com.

CONTRIBUTORS

Meghan Day
Marketing Director, Americas, Diligent Corp.

Catherine Malone
Global Content Marketing Manager, Diligent Corp.

Dottie Schindlinger
Vice President/Governance Technology Evangelist, Diligent Corp.

Kimberly Crowe
Managing Editor, NYSE Governance Services

Melanie C. Nolen
Research Editor, NYSE Governance Services

Deborah Scally
Editor, NYSE Governance Services

NYSE Governance Services